Searching PAJ

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-216046
(43)Date of publication of application : 10.08.2001

(51)Int.Cl. G06F 1/00
G06F 15/00

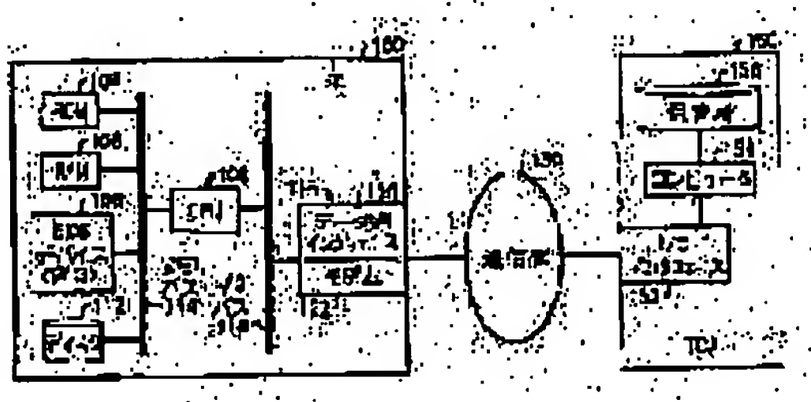
(21)Application number : 2000-371401
(22)Date of filing : 06.12.2000

(71)Applicant : AVAYA TECHNOLOGY CORP
(72)Inventor : THOMPSON JOHN S
THOMPSON MELINDA M

(30)Priority
Priority number : 1999 454625 Priority date : 06.12.1999 Priority country : US

(54) DEVICE SECURITY MECHANISM BASED ON REGISTERED PASSWORD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a security mechanism based on a registered password.
SOLUTION: When a PC is booted, a security program is executed. The security program urges a user to input a password, and this is enciphered by a stored key, and the enciphered password is compared with the stored password. When those passwords are not coincident, the boot is abandoned, and the PC is invalidated. Only when those passwords are coincident, the boot is continued, and the use of the PC is authorized.



LEGAL STATUS

[Date of request for examination]	22.03.2002
[Date of sending the examiner's decision of rejection]	04.04.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）

(12) **公開特許公報（A）**

(11)特許出願公開番号
特開2001－216046
(P2001－216046A)

(43)公開日 平成13年８月10日(2001.8.10)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ	1/00	３７０	Ｇ０６Ｆ	1/00	３７０Ｅ
	15/00	３３０		15/00	３３０Ｅ

審査請求 未請求 請求項の数10 ＯＬ （全 10 頁）

(21)出願番号 特願2000－371401(P2000－371401)

(22)出願日 平成12年12月６日(2000.12.6)

(31)優先権主張番号 ０９／４５４６２５

(32)優先日 平成11年12月６日(1999.12.6)

(33)優先権主張国 米国（ＵＳ）

(71)出願人 500500044
アバイア テクノロジー コーポレーション
アメリカ合衆国. 07920 ニュージャーシィ，バスキング リッジ，マウント エアリー ロード 211

(72)発明者 ジョン エス．トンプソン
アメリカ合衆国 80303 コロラド，ボールダー，エンボリア ロード 695

(72)発明者 メリンダ エム．トンプソン
アメリカ合衆国 80303 コロラド，ボールダー，エンボリア ロード 695

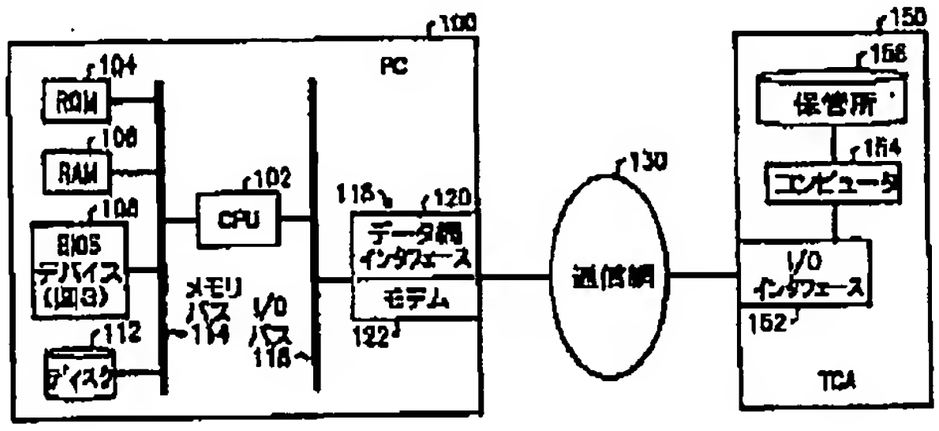
(74)代理人 100064447
弁理士 岡部 正夫 （外11名）

(54)【発明の名称】 登録されているパスワードに基づくデバイス機密機構

(57)【要約】 （修正有）

【課題】 本発明は、登録されているパスワードに基づくデバイス機密機構に関する。

【解決手段】 ＰＣがブートされると、機密プログラムが実行される。機密プログラムは、ユーザにパスワードを催促し、これを格納されている鍵にて暗号化し、暗号化されたパスワードを格納されているパスワードと比較する。これらパスワードが一致しない場合は、ブートは、放棄され、ＰＣは不能にされる。これらパスワードが一致した場合にのみ、ブートが継続され、ＰＣの使用が許される。



【特許請求の範囲】
【請求項１】　デバイス機密装置であって、
パスワードを格納し、およびデバイスの使用が不能にされている間はデバイスのユーザが格納されているパスワードにアクセスすることができないようにするための前記デバイス内のメモリ；前記デバイスを外部エンティティに接続するコネクタ；前記デバイス内の、前記メモリと協力して、ロックに格納されているパスワードと対応するパスワードが与えられない限り、デバイスの使用を不能にするためのロック；および前記メモリ、コネクタ、およびロックと協力して、デバイスの使用が許され、前記外部エンティティへの接続が設定されたことに応答して、前記格納されているパスワードの変更を、前記格納されているパスワードが前記接続された外部エンティティによって格納されているパスワードと一致する場合は、許すとともに、前記外部エンティティによる前記変更されたパスワードの格納を実行するための手段の配列を備えることを特徴とするデバイス機密装置。
【請求項２】　前記メモリが、コンピュータのＢＩＯＳプログラムおよびパスワードを格納するためのＢＩＯＳデバイスから成ることを特徴とするコンピュータ用の請求項１記載の装置。
【請求項３】　前記コネクタが前記デバイスのネットワーク通信ポートから成り；前記エンティティが遠隔信託機関から成ることを特徴とする請求項１記載の装置。
【請求項４】　前記コネクタが前記デバイスの入力ポートから成り；前記エンティティがローカルメモリデバイスから成ることを特徴とする請求項１記載の装置。
【請求項５】　前記ロックが前記デバイスに電力が投入された際に実行する格納されたプログラムから成ることを特徴とする格納プログラム制御方式のデバイス用の請求項１記載の装置。
【請求項６】　前記メモリが、前記コンピュータのＢＩＯＳプログラム、パスワード、およびロックプログラムを格納するためのＢＩＯＳデバイスから成ることを特徴とするコンピュータ用の請求項５記載の装置。
【請求項７】　前記手段の配列が：ユーザの識別を外部エンティティと協力して確立（検証）するための手段；格納されているパスワードを外部エンティティに供給するための手段、および前記外部エンティティからの前記確立（認証）された識別と供給されたパスワードが前記外部エンティティによって格納されている識別とパスワードと一致したことを示す指標の受信に応答して、前記格納されているパスワードの変更を実行するための手段を含むことを特徴とする請求項１記載の装置。
【請求項８】　前記手段の配列がさらに：前記ユーザからの新たなパスワードの受信に応答して、前記メモリ内に新たなパスワードを格納するとともに、前記新たなパスワードを格納のために前記外部エンティティに送信するための手段を含むことを特徴とする請求項７記載の装置。
【請求項９】　前記メモリが、前記パスワードの暗号版および暗号鍵を格納し、
前記ロックが、非暗号化パスワードを受信すると、これに応答して、受信されたパスワードを格納されている暗号鍵にて暗号化し、この暗号版パスワードを前記格納されている暗号版パスワードと比較し、これら比較されたパスワードが一致しない場合は、前記デバイスの使用を不能にすることを特徴とする請求項１記載の装置。
【請求項１０】　前記手段の配列が：ユーザの識別を外部エンティティと協力して確立（検証）するための手段；格納されている暗号版パスワードを前記外部エンティティに供給するための手段；前記外部エンティティからの前記確立（認証）された識別と供給されたパスワードが前記外部エンティティによって格納されている識別とパスワードと一致したことを示す指標の受信に応答して、前記格納されているパスワードの変更を実行するための手段、
外部エンティティから受信される新たな暗号鍵を前記メモリ内に格納するための手段、およびユーザから受信される新たなパスワードを格納されている新たな暗号鍵にて暗号化し、こうして暗号化された新たなパスワードを前記メモリ内に格納するとともに、暗号化された新たなパスワードを格納のために前記外部エンティティに送信するための手段を含むことを特徴とする請求項９記載の装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、一般的には、デバイスの窃盗あるいは無許可のアクセスを抑止するための機密機構、より詳細には、パスワード機構に関する。
【０００２】
【従来の技術】あらゆる種類の電子デバイスは、それらが典型的にサイズの割りに高い価値を有するために窃盗の標的となる。ポータブルコンピュータデバイス、例えば、ノート型コンピュータは、典型的には、小さく、高価で、持運びが楽であるために、特に、盗難に遭い易い。従来の機密対策は、アンカリングデバイスおよびロックエンクロージャを使用する物理的抑止力に基づく。ただし、これらは、運搬性および使用の利便性を制限する。デバイスを所有者以外には使用できないようにし、この事実について宣伝したなら、これらは泥棒にとっては価値を失い、このため、窃盗の対象とはならなくなることが期待できる。これは、暗に簡単には突破することができないある種のパスワードシステムの使用を示唆する。ただし、従来のパスワード機構では不十分である。
【０００３】今日のポータブルコンピュータにおいては、アクセスを制限するためにソフトウエアベースのパスワードシステムが用いられている。ただし、これらは、オペレーティングシステムソフトウエアを再実装す

ることで、あるいは、あるケースにおいては、より単純な操作、例えば、これらをサポートするオペレーティングシステム（例えば、Windows 95における“Safe Mode”）内のループホールに不当に働き掛けることで突破することができる。それにもかかわらず、コンピュータに電力を投入する際にパスワードを供給する方法は、ユーザの正当性をチェックするための最も簡単なやり方である。ハードウエアベースの機密システム（例えば、幾つかのカーラジオ上に搭載されている機密システム）もパスワードによる制御をサポートする。ただし、パスワードが失われた場合は、このデバイスを再び使用できるようにするためには、大変なハードウエアの外科的手術（解体修理）に頼るしかない。パスワードシステムの突破に対するコストおよび労力の両面での障壁を設ける必要があるが、同時に、パスワードが失われた際の扱いが容易であり、しかも、ある機関によってデバイスの正当性を確認できることも要望される。現在、公開暗号署名（Public Encrypted Signatures）が受信された情報がユーザによって合法的に供給されたものであるか検証するために用いられている。割当てられた公開鍵を用いてのパスワードの符号化および暗号化はある人が一意に登録されたデバイスを扱っていることを保障するための手段として用いることができる。信託証明機関（Trusted Certification Authorities、TCA）も存在し、これは、登録されたデジタル署名を提供し、ユーザの登録情報を管理する。これら機関はメッセージの符号化のための署名を登録するために用いることができる。ただし、これら現存の能力（機能／機関）のどれも、それのみでは携帯デバイスに対する十分な機密機構を提供することはできない。

【０００４】

【発明が解決しようとする課題】本出願人は、携帯デバイスに対する機密システムには以下に示すような幾つかの要件が存在することを認識した：

・機密システムは、パーツあるいは製造において、デバイスにあまり大きなコストを追加すべきではなく、できればコストを全く追加すべきではなく、また流通システムにも追加の負担を掛けるべきではない。

・機密システムを突破するための労力もしくは金銭面での費用がデバイスの価値に接近あるいはこれを超過する必要がある。

・デバイスへのアクセスは所有者に個人化され、しかも大きな困難なしに所有権の譲渡が可能である必要がある。

・機密システムは、現存のハードウエア、ソフトウエアおよび機密技術を使用し、好ましくは、現存のコンピュータ上への実装に適したものである必要がある。

・機密システム内で使用される個人的な情報はデバイスへの正当なアクセスを再設定することが必要となったとき支援することができるある機関によって保管できる必要がある。

・機密システムは標準となるのに十分に魅力的であり、デバイスの販売業者と第三者の両方によって経済的にサポートできる必要がある。

【０００５】

【課題を解決するための手段】従って、本発明は、従来の技術のこれら問題および短所を解決するため、および従来の技術の要件を満たすことに向けられる。概略的には、本発明によると、デバイス機密装置は、以下の要素から構成される。第一は、デバイス内の、パスワードを格納するためのメモリである。このメモリは、これが、デバイスのユーザが、デバイスの使用が不能にされている場合は、格納されているパスワードにアクセスすること（つまり、これを抽出および／あるいは変更すること）を防止するできる意味で機密であることを要求される。このようなメモリの一例としては、パーソナルコンピュータのＢＩＯＳプログラムを格納するＢＩＯＳデバイスがある。もう一つの要素は、デバイスを外部エンティティ、例えば、ローカルメモリデバイスもしくは遠隔信託機関に接続するためのコネクタである。このようなコネクタの一例としては、パーソナルコンピュータの入／出力ポートおよびネットワーク通信ポートが含まれる。もう一つの要素は、デバイス内の、メモリと協力して、デバイスの使用を、格納されているパスワードに対応するパスワードがロックに供給されない限り、不能にするロックである。このロックは、一つの実施例においては、機密メモリ、例えば、ＢＩＯＳデバイス内にパスワードとともに存在するプログラムとして実現される。もう一つの要素は、メモリ、コネクタ、およびロックと協力して、デバイスの使用が許され、外部エンティティへの接続が設定されたことに応答して、格納されているパスワードが接続された外部エンティティによって格納されているパスワードと一致したとき、格納されているパスワードの変更を許すとともに、外部エンティティによる変更されたパスワードの格納を実行するための手段の配列である。この手段の配列は、一つの実施例においてはプログラムとして実現されるが、ただし、これは必ずしも機密デバイスに格納される必要はない。

【０００６】本発明は、

【発明が解決しようとする課題】のセクションにおいて指摘された幾つかのあるいは全ての要件が満たされるように実現される。これら要件には上述のように以下が含まれる：

１．製造過程において、他のソフトウエアをインストールするために非機密始動モードを選択できる要件。

２．機密システムの突破には、デバイスを解体し、機密メモリ（例えば、コンピュータのＢＩＯＳメモリ）を物理的に切り離し、書きなおすことが要求される要件。これは、簡単で安価な仕事ではない。

３．デバイスの所有権を個人化するばかりではなく、こ

れを安全に譲渡もしくは変更できる要件。
４．新たな技術を必要としないという要件。実際、本発明の機能は、現存の知能デバイス、例えば、コンピュータに追加することもできる。
５．信託機関を、機密を管理および制御するため、および価値あるサービスを提供するために使用できるという要件。信託機関の代わりに、信託機関の代わって機能し、システムのよりローカルなバージョンを提供するために、ＰＣカードのようなローカルプラグインデバイスを使用することもできる。
６．本発明は、上述の全ての要件を満たすように実現できるために、本発明は標準としておよび／あるいは広く展開された商業的機能として魅力的である。本発明のこれらおよびその他の特徴および長所が、本発明の実施例の以下の説明を図面を参照しながら読むことで一層明白になるものである。
【０００７】
【発明の実施の形態】図１は、ポータブルコンピュータ（ＰＣ）１００を示す。ポータブルコンピュータ（ＰＣ）１００は、中央演算ユニット（ＣＰＵ）１０２、読出専用メモリ（ＲＯＭ）１０４、ランダムアクセスメモリ（ＲＡＭ）１０６、ベーシック入／出力オペレーティングシステム（ＢＩＯＳ）デバイス１０８、およびディスクメモリ１１２を備え、これら全てがメモリバス１１４によって相互接続される。ポータブルコンピュータ（ＰＣ）１００は、さらに、入／出力（Ｉ／Ｏ）インタフェース１１６を備え、これは、データ網インタフェース１２０および／あるいはモデム１２２から成り、入／出力（Ｉ／Ｏ）バス１１８によって中央演算ユニット（ＣＰＵ）１０２に接続される。図２には、入／出力（Ｉ／Ｏ）インタフェース１１６が入／出力（Ｉ／Ｏ）ポート２２０から成るポータブルコンピュータ（ＰＣ）１００の代替の形態が示される。上の説明までは、ポータブルコンピュータ（ＰＣ）１００は従来のものである。ポータブルコンピュータ（ＰＣ）１００は、ＢＩＯＳデバイス１０８のようなメモリ要素：すなわち、その内容がデバイスの動作が不能にされている際はデバイスのユーザによって容易にアクセス（抽出もしはく変更）すること、あるいはバイパスすることは不可能であり、その動作能力がこれらの内容に依存するメモリ要素をもつ任意のデバイスであり得る。
【０００８】ＢＩＯＳデバイス１０８は、不揮発性の"永久(permanent)"メモリから成り、この内容は、電力が不在のときも保存される。ただし、読出専用メモリ（ＲＯＭ）１０４とは異なり、これは、特別なソフトウエアの制御の下で、電気的に変更およびプログラムが可能であり、ポータブルコンピュータ（ＰＣ）１００の寿命を通じてＢＩＯＳ１０８を更新することができる。このタイプのメモリデバイスは、プログラム可能読出専用メモリ（ＰＲＯＭ）、電気的消去可能ＰＲＯＭ（ＥＥＰＲＯＭ）もしくはフラッシュメモリとして知られている。ポータブルコンピュータ（ＰＣ）１００がブートされると、例えば、電力が投入されると、中央演算ユニット（ＣＰＵ）１０２が読出専用メモリ（ＲＯＭ）１０４からのインストラクションの実行を開始する。これらインストラクションは、中央演算ユニット（ＣＰＵ）１０２に対して、ＢＩＯＳ１０８の内容（ＢＩＯＳプログラム）をランダムアクセスメモリ（ＲＡＭ）１０６内に転送し、ランダムアクセスメモリ（ＲＡＭ）１０６からのこれら内容を実行するように指令する。ＢＩＯＳプログラムの実行によってポータブルコンピュータ（ＰＣ）１００がブートされる。ポータブルコンピュータ（ＰＣ）１００は、ＢＩＯＳプログラムなしではブートすることはできない。そして、もし、ポータブルコンピュータ（ＰＣ）１００がブートできない場合は、ＢＩＯＳプログラムは更新することも変更することもできない。このため、ＢＩＯＳデバイス１０８の内容が"コラプト（corrupted）"した場合は、ＢＩＯＳデバイス１１８を交換するか、ポータブルコンピュータ（ＰＣ）１００を製造業者にもってゆき、ＢＩＯＳデバイス１０８への通常の電気接続を物理的にバイパスし、これを再プログラムすることが必要となる。これも従来のやり方である。
【０００９】図３は、ＢＩＯＳデバイス１０８の内容を示す。本発明によると、ＢＩＯＳデバイス１１８は、窃盗抑止のための機密機構を実装する。従来のＢＩＯＳプログラム３００を含むことに加えて、ＢＩＯＳデバイス１０８は、暗号鍵３０４およびパスワード３０６の項目を含む機密プログラム３０２も含む。機密プログラム３０２は、ＢＩＯＳプログラムの先頭に付加され、ブート時に、これがランダムアクセスメモリ（ＲＡＭ）１０６内に、ＢＩＯＳプログラム３００の前にあるいはこれとともにロードされ、ＢＩＯＳプログラムの実行が完結される前に実行される。
【００１０】機密機構の基本概念は、ＢＩＯＳデバイス１０８内に一意なパスワード３０６を格納しておき、各ブート（例えば、電力の投入）サイクルの最初に、ブートサイクルおよびその後のポータブルコンピュータ（ＰＣ）１００の動作を続けるためには、キーボードあるいは他のＩ／Ｏデバイスから入力されたパスワード３０６がこれと一致することを要求することにある。パスワード３０６の不一致は、機能的には、ＢＩＯＳプログラム３００の"コラプト（corrupt）"と等価となる。このため、ポータブルコンピュータ（ＰＣ）１００は、パスワード３０６をもたないものによってはなんの役にも立たなくなる。そして、この機密機構を出し抜くことは非常に困難である。これには、ＢＩＯＳデバイス１０８を新たなものと交換するか、ポータブルコンピュータ（ＰＣ）１００を製造業者にもってゆき、ＢＩＯＳデバイス１０８への通常の電気的接続を物理的にバイパスし、これを再プログラムすることが必要となる。このため、ポ

ータブルコンピュータ（ＰＣ）１００を盗むことは経済的な価値がなくなり、このため窃盗の抑止となる。

【００１１】一方において、機密機構は、これを出し抜くもしくは突破することが努力に値しなくなるのに十分にロバスト（頑丈）であることが要求され、他方においては、この機密機構は、パスワードを忘れてしまった場合にもマシーンの使用を回復でき、または、パスワードを見破られたり、マシーンが合法的に人手に渡った場合でも、機密を回復できるように十分に柔軟であることが要求される。この目的のために、ＴＣＡ（trusted certification authority：委託証明機関）１５０の概念が導入される（図１参照）。

【００１２】ＴＣＡ１５０は、パスワードの保管所であるとともに、パスワードの維持に対するサービスでもある。これは、例えば、ポータブルコンピュータ（ＰＣ）１００の製造業者もしくは販売業者による顧客へのサービスとして、あるいは第三者による有料加入サービスとして提供される。図１に示すように、ＴＣＡ１５０は、ＴＣＡ１５０とＰＣ１００が通信することを可能にする通信網１３０（例えば、データ網もしくは電話網）への入／出力（Ｉ／Ｏ）インタフェース１５２、ＴＣＡサービスプログラムを実行するコンピュータ１５４、およびパスワードおよび関連する情報を格納するための保管所１５６（例えばデータベース）から構成される。

【００１３】図２に示す代替の実施例においては、中央ＴＡＣ１５０が省かれ、各ＰＣ１００に、ＴＣＡ一代用機能をその対応するＰＣのみに提供する機密カード２５０が設けられる。機密カード２５０は、ＰＣ１００のＩ／Ｏポート２２０と着脱可能に噛み合う（例えば、これらプラグインされる）Ｉ／Ｏポート２５２とメモリ２５４から構成される。これは、一例においては、ＰＣＭＣＩＡカードあるいはフロッピー（登録商標）ディスクから成る。

【００１４】新しく製造されたＰＣ１００は、これがその内部に搭載された有効なパスワードをもたず、パスワード３０６がナル値であるという意味で機密ではない。このように機密でないモードにあるために、ＰＣ１００は、工場においてなんの障害もなく、ソフトウエアにて初期化し、テストすることができる。さらに、ＰＣ１００は、有効なパスワードなしに販売することもできる。ただし、ＰＣ１００は、エンドユーザに販売する前のＰＣ１００の窃盗を抑止するために、工場から出荷する前に有効なパスワード３０６にてプログラムしておくこともできる。後者の場合は、販売の時点でパスワードを顧客に伝えることとともに、パスワード３０６あるいはＰＣ１００の所有者を識別する情報をＴＣＡ１５０の保管所１５６内に入力しておくか、できるだけ早くパスワード３０６を機密カード２５０のメモリ１５６内に入力することが必要となる。

【００１５】図４～図６は、機密プログラム３０２の機能を示す。例えば、電力が投入されたために、ステップ４００において、ＢＩＯＳデバイス１０８の内容の実行が開始されると、ＣＰＵ１０２は、ステップ４０１において、ＰＣ１００のディスプレイおよびキーボードを起動する。殆どのＢＩＯＳプログラム３００は、基本的なディスプレイおよびキーボードドライバを備えるために、ステップ４０１は、通常は、ＢＩＯＳプログラム３００のディスプレイおよびキーボードを起動する部分を実行することから成る。キーボードおよびディスプレイを動作を起動しないＢＩＯＳプログラム３００の場合は、ステップ４０１は、機密プログラム３０２の基本的なディスプレイおよびキーボードドライバを含む部分、あるいはディスクからディスプレイおよびキーボードドライバをロードし、これらを起動する部分を実行することから成る。次に、ステップ４０２において、ＣＰＵ１０２が、プログラム３０２を実行し、最初に、パスワード３０６をチェックし、その値がナルであるか否か決定する。この値がナルでない場合は、ＰＣ１００は、機密モードにて動作しており、このため、ＣＰＵ１０２は、ステップ４０４において、ＰＣ１００のユーザにパスワードを入力するように催促する。これは、例えば、ＰＣ１００のディスプレイ画面にこの効果のためのプロンプトを表示することによって行なわれる。ユーザがこれに応答すると、例えば、ＰＣ１００のキーボードを用いてパスワードをタイプ入力すると、ＣＰＵ１０２は、ステップ４０６において、受信されたパスワードを格納されている暗号鍵３０４にて暗号化し、次に、ステップ４０８において、暗号化された受信されたパスワードを、これも暗号鍵３０４にて暗号化されたパスワード３０６と比較し、それらが一致するか決定する。これらが一致しない場合は、ステップ４１０において、ＰＣ１００のブートおよびそれ以上の動作を中止し、ＰＣ１００を使用できないようにする。これらが一致した場合は、ＰＣ１００は、安全であり、このため、ステップ４１１において、ＰＣ１００のブーティングを完結させる。ただし、制御を放棄する前に、ステップ４１２において、プログラム３０２は、ＣＰＵ１０２に対して、ユーザにパスワードの変更を希望するか尋ねることを指令する。ステップ４１２においてユーザがパスワードの変更を希望しないことが決定された場合は、ＰＣ１００は、ステップ４２０において、従来のやり方で、ただし、機密モードにて動作を継続する。

【００１６】ステップ４０２に戻り、ここでパスワード３０６がナルであることが決定された場合は、これは、ＰＣ１００が非機密モードにて動作していることを意味し、このため、ＣＰＵは、ステップ４１５において、ブーティングを完結させる。ただし、制御を放棄する前に、プログラム３０２は、ステップ４１６において、ＣＰＵ１０２に対して、ユーザに有効なパスワードの設定を催促するように指令する。ステップ４１８においてユ

ーザがパスワードの設定を選択しないことが決定された場合は、ＰＣ１００は、ステップ４２０において、従来のやり方で非機密モードにて動作を継続する。

【００１７】機密機構が突破されないようにするためには、ＰＣの動作能力を起動あるいは不能にする（制御する）機密ゲートウェイもしくはロックを構成する機密プログラム３０２のステップ４０２～４１０のみをバイパスあるいは突破から保護することで十分である。従って、プログラム３０２のこの部分のみが、パスワード３０６および暗号鍵３０４とともに、機密メモリ、例えば、ＢＩＯＳデバイス１０８内に格納される。その後は、機密ゲートウェイは、パスワード３０６の値がナルの場合、もしくは正しいパスワードが入力された場合に通過できる。いずれの場合も、ユーザは、現在、ＰＣ１００を所望のやり方で自由に用いることができる。従って、プログラム３０２の、単にパスワード３０６の変更（初期設定も含む）を制御する残りの部分は、ＣＰＵ１０２によってアクセスできるＰＣ１００の任意の他の部分に格納することができる。例えば、フロッピーディスクがディスクドライブ内に存在する場合は、ＢＩＯＳプログラム３００は、ＰＣにおいて通常行なわれるようにこれからブートすることを試み、このため、プログラム３０２の残りの部分はフロッピーディスク上に格納され、この時点で、パスワード３０６を設定もしくは修正するために実行される。後に説明するように、パスワードの維持は、ＢＩＯＳデバイス１０８の二つの項目３０４と３０６のみが変更される点とＰＣ１００の外部への通信が行なわれる点を除いて、機能的にはＢＩＯＳプログラム３００のグレードアップあるいは変更と差はない。

【００１８】図面に戻り、図４のステップ４１４においてユーザがパスワードの変更を選択した場合、あるいはステップ４１８においてパスワードの設定を選択した場合は、ＣＰＵ１０２は、図５におけるＴＣＡ１５０あるいは図６における機密カード２５０との対話へと進む。最初に、図５に進み、ＣＰＵ１０２は、ステップ４２４において、従来のやり方で、ＴＣＡ１５０への接続を網インタフェース１２０およびデータ網１３０（例えば、ＬＡＮもしくはインターネット）あるいはモデム１２２および電話網１３０を介して設定する。ＴＣＡ１５０の必要なアドレスは、機密プログラム３０２の一部として格納されるか、あるいは、ステップ４２２において、ＣＰＵ１０２がユーザにアドレスを供給するように催促することで得られる。ステップ２５０において接続が設定されると、ステップ４２６と４５２において、ＰＣ１００とＴＣＡ１５０が協力して、発呼ユーザの識別を確立（検証）する。例えば、ＴＣＡ１５０が網１３０を介してユーザに質問し、ユーザがＰＣ１００を介してこれらに答え、ＴＣＡ１５０が、これら答えを保管所内に格納してあるそのユーザに関する情報と比較し、一致が見られるか決定する。別の方法として、ステップ４２６と４５２は、現存のパスワードの変更の場合は省略することもできる。ユーザの識別がＴＣＡ１５０を満足させるように確立（認証された）場合は、ＴＣＡ１５０は、ステップ４５４において、ＰＣ１００の格納されている暗号版パスワード３０６を要求し、ＣＰＵ１０２は、これに応じて、ステップ４２８において、パスワード３０６を検索し、これを送り返す。受信されたパスワードが、ステップ４５５において、ナルでないことが決定された場合は、ＴＣＡ１５０はステップ４５６において、保管所１５６を探索し、このパスワードおよびこれと対にしてこれと関連して格納されているユーザの識別を含む任意の情報を見つける。保管所１５６内にパスワードが見つかった場合は、ＴＣＡ１５０は、ステップ４５８において、そのペアの情報がステップ４５２において決定された発呼ユーザの識別と一致するか決定する。格納されている識別と発呼ユーザの識別が一致しない場合は、ＴＣＡ１５０は、ステップ４６０において、ＰＣ１００にその通知およびやりとりの拒否を送信し、ステップ４６２において、ＰＣ１００への接続を切ることでこのやりとりを終了する。代替として、（パスワードの変更であり）ステップ４２６と４５２が遂行されない場合は、ＴＣＡ１５０は、単に、ステップ４５６において、受信されたパスワードを求めて保管所１５６を探索し、ステップ４５８において、保管所１５６内にそのパスワードが存在するかチェックする。ＣＰＵ１０２が、ステップ４３０において、そのやりとりが拒否されたことを決定した場合、ＣＰＵ１０２は、ステップ４３２において、パスワードの変更を行なうことなく、従来の動作を継続する。別の方法として、ＣＰＵ１０２は、ステップ４３２において、ブートアップを否定し、ＰＣ１００を停止し、こうして、ＰＣ１００を使用ではないようにすることもできる。

【００１９】ステップ４５８において、発呼ユーザの識別がこのＰＣ１００のパスワード３０６としてＴＣＡ１５０によって格納されているユーザの識別と一致することが見つかった場合、もしくは、ステップ４５５において、受信されたパスワードがナルであることが見つかった場合は、ＴＣＡ１５０は、ステップ４６６において、新たなプライベート／公開暗号鍵ペアを生成し、ステップ４６８において、このペアの公開暗号鍵をＰＣ１００に送信する。ＣＰＵ１０２は、ステップ４３６において、この公開暗号鍵を受信し、ステップ４３８において、これを、ＢＩＯＳデバイス１０８の暗号鍵３０４内に格納し、このプロセス内の暗号鍵３０４の以前の値を無効にする。ＣＰＵ１０２は、次に、ステップ４４０において、ユーザに新たなパスワードを催促し、これを受信すると、ステップ４４２において、この新たなパスワードを格納されている暗号鍵３０４にて暗号化する。ＢＩＯＳデバイス１０８をプログラミングするための従来

の専用のソフトウエアの制御下において、ＣＰＵ１０２は、次に、ステップ４４４において、新に暗号化されたパスワードをＢＩＯＳ１０８のパスワード３０６内に格納し、このプロセスにおけるパスワード３０６の以前の値を無効にする。幾つかのＢＩＯＳデバイスは、その内容を変更するためには、全デバイスを無効にすることを要求することがあり、この場合は、ＴＣＡ１５０が全ＢＩＯＳデバイスに新たな暗号鍵とパスワードをもつ内容を供給するか、もしくは、ＣＰＵ１０２が、ＢＩＯＳデバイスの内容を読み出し、そのイメージを生成し、そのイメージ内の暗号鍵およびパスワードを変更し、その後、変更されたイメージを再びＢＩＯＳデバイス内に書き込むことが必要となる。このため、ＣＰＵ１０２は、ステップ４４６において、新たな暗号版パスワードをＴＣＡ１５０に送信する。ＰＣ１００は、次に、ステップ４４８において、従来の動作に進む。TCA１５０は、ステップ４７０において、新たな暗号版パスワードを受信し、ステップ４７２において、これと新に生成された暗号鍵ペアのプライベート鍵を、保管所１５６内に、発呼者識別情報と関連する以前のパスワードと鍵の代わりに、格納する。ＴＣＡ１５０は、次に、ステップ４７４において、その動作を終了する。

【００２０】ユーザが万一パスワードを忘れてしまった場合は、ユーザは、これをＴＣＡ１５０の助けを借りて検索することができる。例えば、ユーザは、ＴＣＡ１５０の運用者に電話を掛け、ステップ４２６と４５２のやり方で、運用者に対してユーザの識別を確立する。保管所１５６内に格納されているユーザに関する情報にはユーザの声紋が含まれ、運用者は、この声紋と電話のユーザの音声とを用いて、ユーザを認証することができる。いったんユーザが認証されると、運用者は、コンピュータ１５４に対して、ユーザのパスワードを解読するように指令する。コンピュータ１５４は、これを、保管所１５６からユーザの暗号版パスワードおよびプライベート暗号鍵を探索し、プライベート鍵を用いてこのパスワードを解読することによって行なう。運用者は、次に、解読されたパスワードを呼を介してユーザに報告し、同時に、呼が機密でない場合は、できる限り早くパスワードを変更するように警告する。

【００２１】ＰＣ１００のユーザが、図２の実施例の場合のように、機密カード２５０を搭載する場合は、ステップ４１３においてパスワードの変更が選択された場合、もしくはステップ４１８においてパスワードの設定が選択された場合、ＣＰＵ１０２は、図６に示すやり方で、機密カード２５０との対話を開始する。最初に、ＣＰＵ１０２は、ステップ６００において、Ｉ／Ｏポート２２０内に機密カード２００が存在するかチェックする。機密カード２５０がＩ／Ｏポート２２０に接続されてない場合は、ＣＰＵ１０２は、ステップ６０２において、ＰＣ１００のユーザに接続することを催促し、次に、ステップ６００に戻る。ステップ６００において、機密カード２５０がＩ／Ｏポート２２０に接続されていることが決定された場合は、ＣＰＵ１０２は、オプションとして、ステップ６０４～６０８において、別のデバイスに対するパスワードを誤って破壊することを防止するために、それがこのＰＣ１００に対して正しい機密カードであるか否かチェックする。このチェックを遂行するために、ＣＰＵ１０２は、ステップ６０４において、機密カード２５０からメモリ２５４の内容を検索し、ステップ６０６において、これら内容をパスワード３０６と比較し、それらが一致するか調べる。一致しない場合は、ＣＰＵ１０２は、ステップ６０８において、ユーザに対して、正しい機密カード２５０をＰＣ１００に接続するように催促し、その後、ステップ６００に戻る。ＣＰＵ１０２がステップ６０６において正しい機密カード２５０がＰＣ１００に接続されていることを見つけた場合、もしくは機密カード２５０が正しいものであるかチェックするためのステップ６０４～６０８が省略される場合は、ＣＰＵ１０２は、ステップ６１０において、ユーザに新たなパスワードを催促し、これを受信する。ＣＰＵ１０２は、次に、ステップ６１２において、暗号鍵３０４を用いて、この新たなパスワードを暗号化する。公開鍵の暗号化は、ＴＣＡ１５０などの遮隔機関は存在しないために不要である。オプションとして、例えば、殆どのＵＮＩＸ（登録商標）オペレーティングシステム環境において通常見られるように、全てのＰＣ１００内に共通の鍵を用いることもできる。ＢＩＯＳデバイス１０８をプログラミングするための従来の専用のソフトウエアの制御下において、ＣＰＵ１０２は、次に、ステップ６１４において、新に暗号化されたパスワードを、ＢＩＳＯデバイス１０８内にパスワード３０６として格納する。ＣＰＵ１０２は、さらに、ステップ６１６において、これを、機密カード２５０のメモリ２５４内に、ここに格納されている以前の内容の代わりに、格納する。図５のステップ４４４の場合と同様に、機密カード２５０は、全ＢＩＯＳデバイス１０８の内容を新たなパスワードとともに供給することが必要とされる場合がある。代替もしくは追加として、ＣＰＵ１０２は、機密カード２５０のメモリ２５４内に非暗号化パスワードを格納することもできる。この方法は、ユーザが万一パスワードを忘れてしまった場合でも、ユーザがこれを機密カード２５０からコンパティブルなＩ／Ｏポート２２０をもつ別のマシーンを介して検索できる（読出しおよび／あるいは表示できる）という長所をもつ。ただし、これは、ユーザが機密カード２５０を、ＰＣ１００とは別個に、物理的に機密に保つことを期待できることを仮定する。ＣＰＵ１０２は、その後、従来のやり方で動作を継続する。勿論、当業者においては明らかなように上述の実施例に対する様々な変更および修正が可能である。例えば、本発明は、様々な異なるデバイス上に、ある一つの

実現の機密が突破された場合でも全てのデバイスが影響を受けることがないように異なるやり方にて（例えば、製造業者に特定な、さらに、モデルに特定なやり方にて）実現することもできる。この目的に対しては、デバイス（ＰＣ）の通し番号がＲＯＭ１０４内に格納され、これが製造業者および／あるいはモデルを識別するために用いられる。これら変更および修正は、本発明の精神および範囲から逸脱することも、本発明の付随する長所を低減することもなく、実施することが可能であり、従って、これら変更および修正も、従来の技術によって制限されない限り、特許請求の範囲内に含まれるものである。

【図面の簡単な説明】

【図１】本発明の第一の実施例を含むコンピュータ網のブロック図である。

【図２】本発明の第二の実施例を含むコンピュータ網のブロック図である。

【図３】図１および図２のポータブルコンピュータのＢＩＯＳデバイスの内容のブロック図である。

【図４】一体となって、図１および図２のポータブルコンピュータの機密プログラムの動作の機能流れ図である。

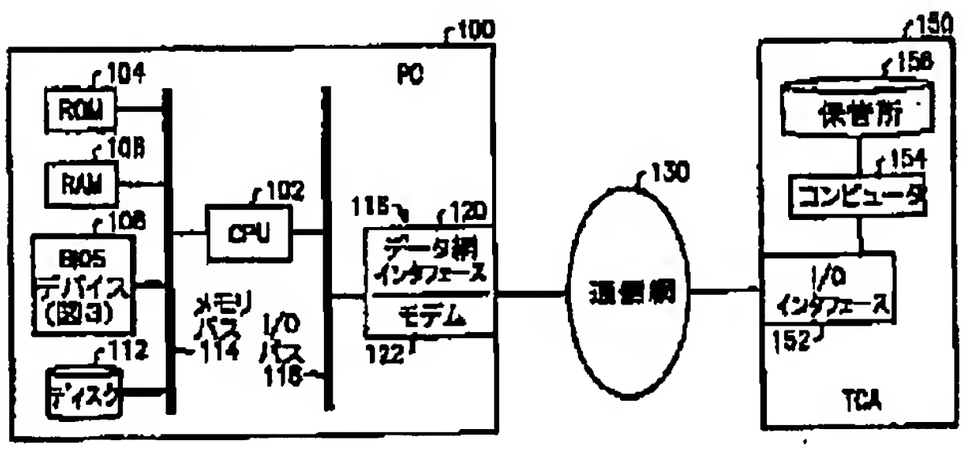
【図５】図１のコンピュータ網の信託証明機関の動作の機能流れ図である。

【図６】一体となって、図１および図２のポータブルコンピュータの機密プログラムの動作の機能流れ図である。

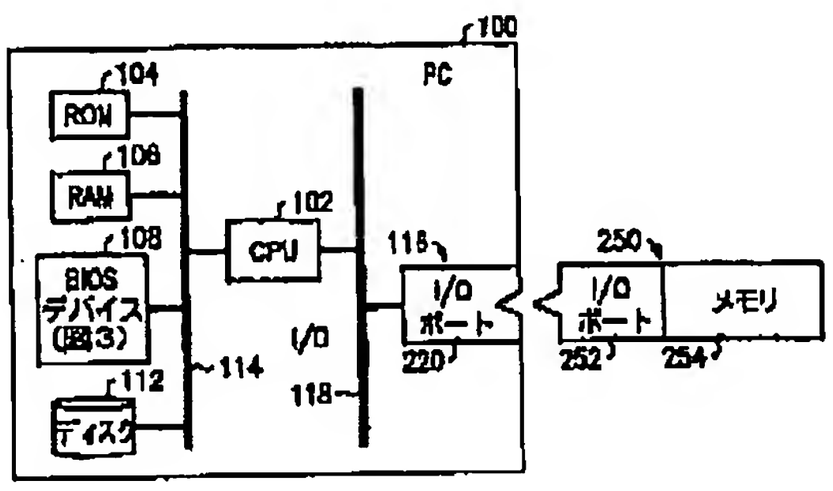
【符号の説明】

１００　ポータブルコンピュータ（ＰＣ）
１０２　中央演算ユニット（ＣＰＵ）
１０４　読出専用メモリ（ＲＯＭ）
１０６　ランダムアクセスメモリ（ＲＡＭ）
１０８　ベーシック入／出力オペレーティングシステム（ＢＩＯＳ）デバイス
１１２　ディスクメモリ
１１４　メモリバス
１１６　入／出力（Ｉ／Ｏ）インタフェース
１１８　入／出力（Ｉ／Ｏ）バス
１２０　データ網インタフェース
１２２　モデム
１３０　通信網
１５０　ＴＣＡ（委託証明機関）
１５２　入／出力（Ｉ／Ｏ）インタフェース
１５４　コンピュータ
１５６　保管所
２２０　入／　出力（Ｉ／Ｏ）ポート
２５０　機密カード
２５２　Ｉ／Ｏポート
２５４　メモリ
３００　ＢＩＯＳプログラム
３０２　機密プログラム
３０４　暗号鍵
３０６　パスワード

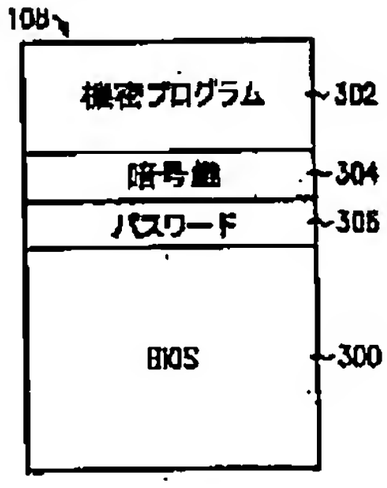
【図１】



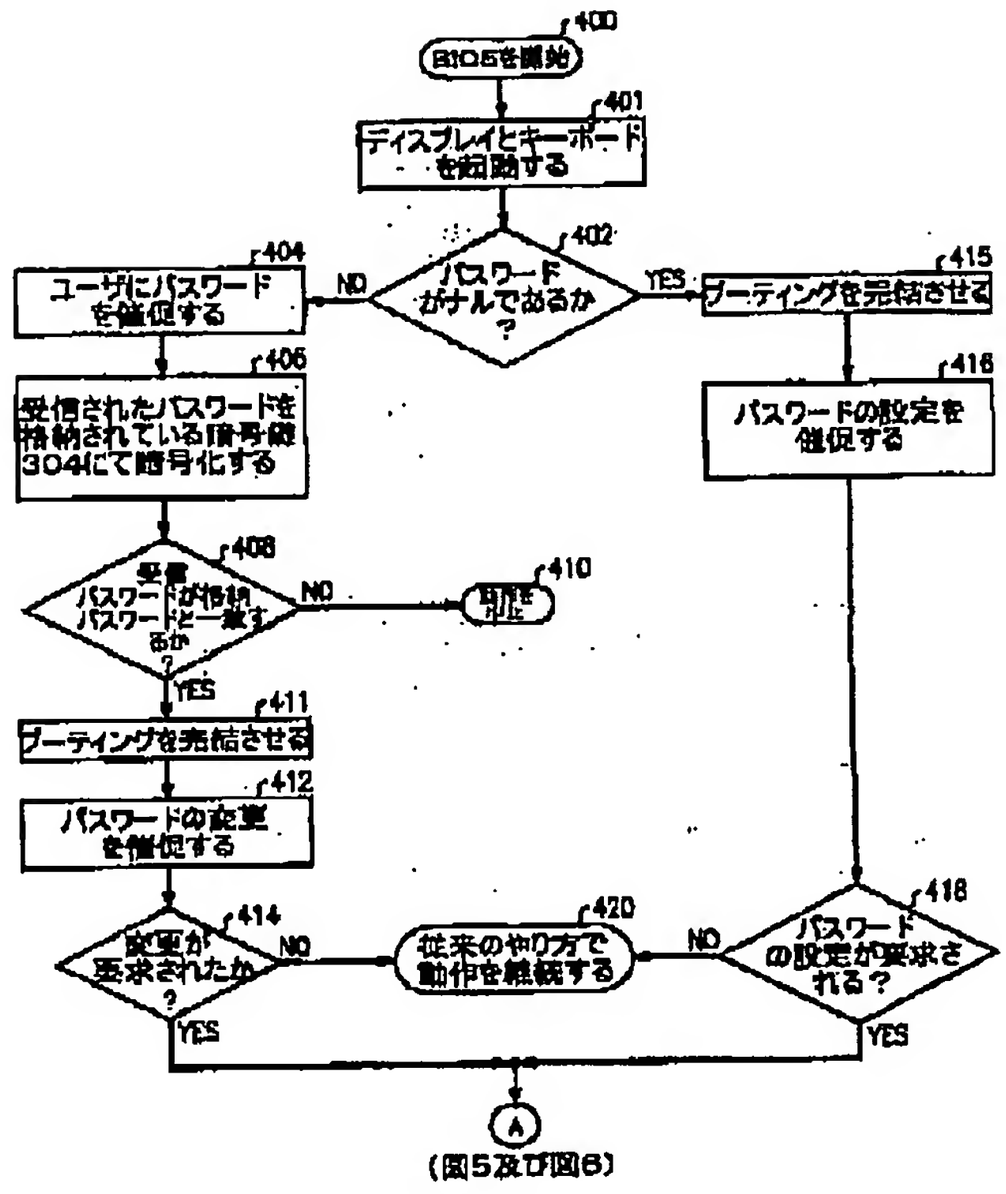
【図２】



【図３】

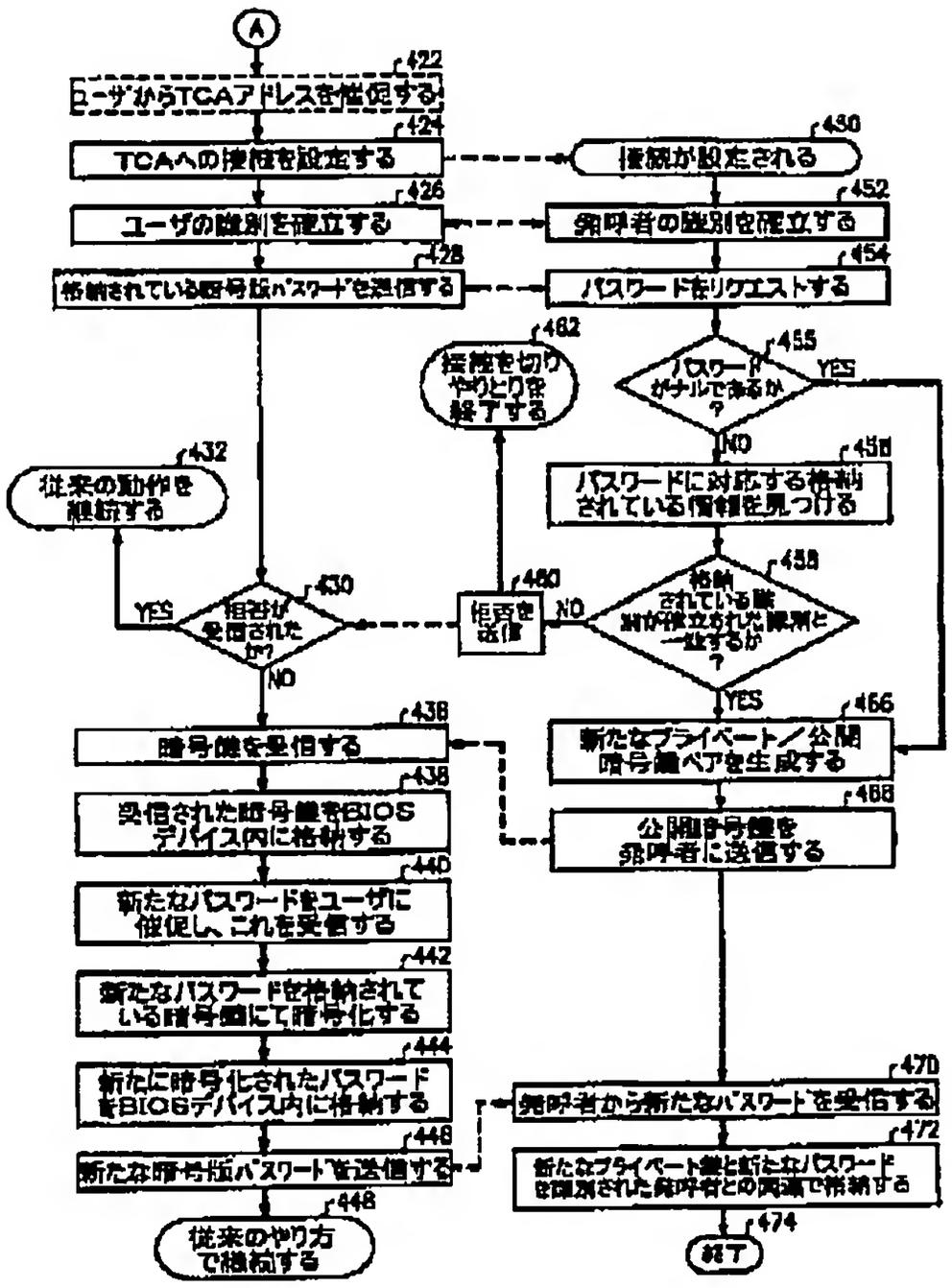

108
機密プログラム
302
暗号鍵
304
パスワード
306
BIOS
300

【図４】

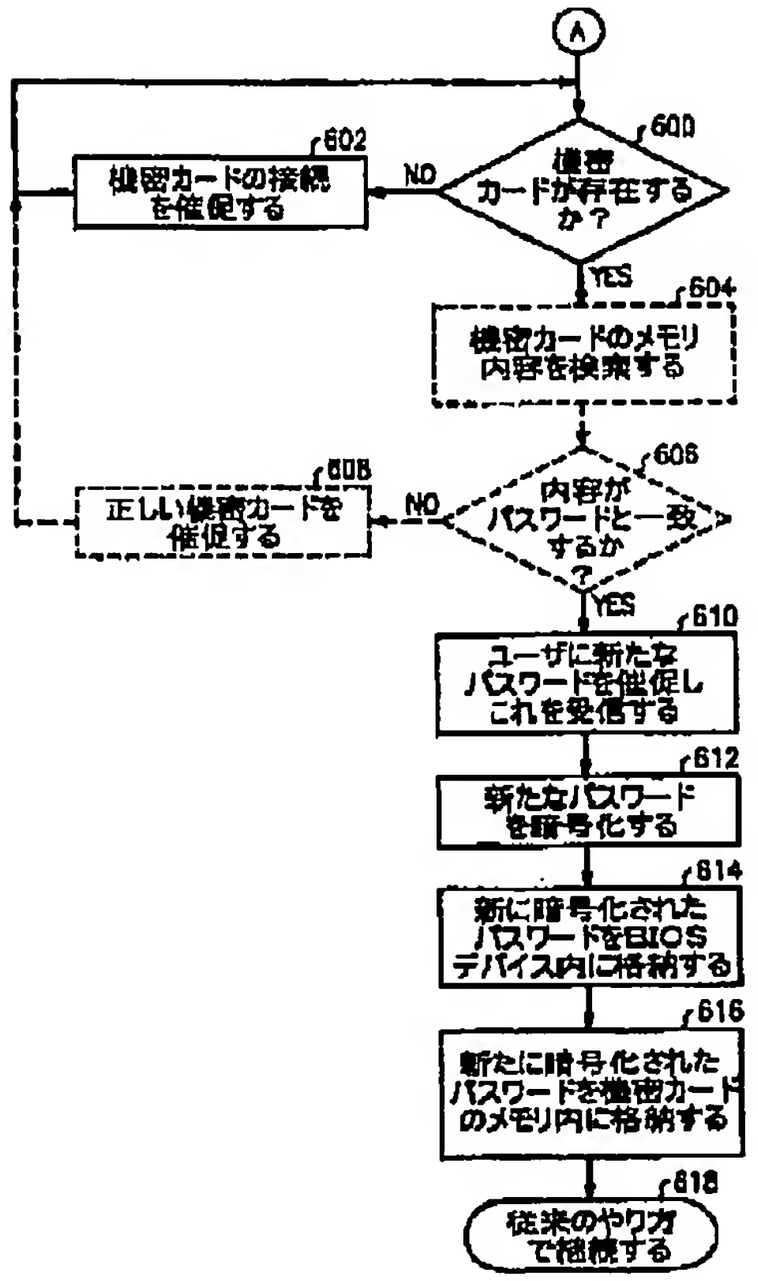

400
BIOSを開始
401
ディスプレイとキーボードを初期化する
402
パスワードがナルであるか？
NO
YES
404
ユーザにパスワードを催促する
406
受信されたパスワードを格納されている暗号鍵304にて暗号化する
408
受信パスワードが格納パスワードと一致するか？
NO
410
YES
411
ブーティングを完結させる
412
パスワードの設定を催促する
414
設定が要求されたか？
NO
420
従来のやり方で動作を継続する
415
ブーティングを完結させる
416
パスワードの設定を催促する
418
パスワードの設定が要求される？
NO
YES
YES
A

（図５及び図６）

【図５】



【図６】



【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成１４年６月２６日（２００２．６．２６）

【公開番号】特開２００１－２１６０４６（Ｐ２００１－２１６０４６Ａ）
【公開日】平成１３年８月１０日（２００１．８．１０）
【年通号数】公開特許公報１３－２１６１
【出願番号】特願２０００－３７１４０１（Ｐ２０００－３７１４０１）
【国際特許分類第７版】
　Ｇ０６Ｆ　1/00　370
　　15/00　330
【Ｆ Ｉ】
　Ｇ０６Ｆ　1/00　370 Ｅ
　　15/00　330 Ｅ

【手続補正書】
【提出日】平成１４年３月２２日（２００２．３．２２）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　デバイスセキュリティ装置であって、パスワードを格納し、およびデバイスの使用が不能にされている間はデバイスのユーザが格納されているパスワードにアクセスすることができないようにするための前記デバイス内のメモリ；
前記デバイスを外部エンティティに接続するコネクタ；
前記デバイス内の、前記メモリと協力して、ロックに格納されているパスワードと対応するパスワードが与えられない限り、デバイスの使用を不能にするためのロック；および
前記メモリ、コネクタ、およびロックと協働する配列であって、デバイスの使用が許され、前記外部エンティティへの接続が設定されたことに応答して、前記格納されているパスワードの変更を、前記格納されているパスワードが前記接続された外部エンティティによって格納されているパスワードと一致する場合は、許すとともに、前記外部エンティティによる前記変更されたパスワードの格納を実行するための配列を備えることを特徴とするデバイスセキュリティ装置。
【請求項２】　前記メモリが、コンピュータのＢＩＯＳプログラムおよびパスワードを格納するためのＢＩＯＳデバイスから成ることを特徴とするコンピュータ用の請求項１記載の装置。
【請求項３】　前記コネクタが前記デバイスのネットワーク通信ポートから成り：
前記エンティティが遠隔信託機関から成ることを特徴とする請求項１記載の装置。
【請求項４】　前記コネクタが前記デバイスの入力ポートから成り；前記エンティティがローカルメモリデバイスから成ることを特徴とする請求項１記載の装置。
【請求項５】　前記ロックが前記デバイスに電力が投入された際に実行する格納されたプログラムから成ることを特徴とする格納プログラム制御方式のデバイス用の請求項１記載の装置。
【請求項６】　前記メモリが、前記コンピュータのＢＩＯＳプログラム、パスワード、およびロックプログラムを格納するためのＢＩＯＳデバイスから成ることを特徴とするコンピュータ用の請求項５記載の装置。
【請求項７】　前記の配列が：ユーザの識別を外部エンティティと協力して確立するための手段；
格納されているパスワードを外部エンティティに供給するための手段、および前記外部エンティティからの前記確立された識別と供給されたパスワードが前記外部エンティティによって格納されている識別とパスワードと一致したことを示す指標の受信に応答して、前記格納されているパスワードの変更を実行するための手段を含むことを特徴とする請求項１記載の装置。
【請求項８】　前記配列がさらに：
前記ユーザからの新たなパスワードの受信に応答して、前記メモリ内に新たなパスワードを格納するとともに、前記新たなパスワードを格納のために前記外部エンティティに送信するための手段を含むことを特徴とする請求項７記載の装置。
【請求項９】　前記メモリが、前記パスワードの暗号版および暗号鍵を格納し、
前記ロックが、非暗号化パスワードを受信すると、これに応答して、受信されたパスワードを格納されている暗号鍵にて暗号化し、この暗号版パスワードを前記格納されている暗号版パスワードと比較し、これら比較されたパスワードが一致しない場合は、前記デバイスの使用を

不能にすることを特徴とする請求項１記載の装置。

【請求項１０】　前記手段の配列が：

ユーザの識別を外部エンティティと協力して確立するための手段；

格納されている暗号版パスワードを前記外部エンティティに供給するための手段；

前記外部エンティティからの前記確立された識別と供給されたパスワードが前記外部エンティティによって格納されている識別とパスワードと一致したことを示す指標の受信に応答して、前記格納されているパスワードの変更を実行するための手段、

外部エンティティから受信される新たな暗号鍵を前記メモリ内に格納するための手段、および

ユーザから受信される新たなパスワードを格納されている新たな暗号鍵にて暗号化し、こうして暗号化された新たなパスワードを前記メモリ内に格納するとともに、暗号化された新たなパスワードを格納のために前記外部エンティティに送信するための手段を含むことを特徴とする請求項９記載の装置。